REMARKS

Claims 25, 27 and 28 have been amended. Claim 29 has been added.

The Examiner has rejected applicant's claims 25-28 under 35 USC § 102(b) as anticipated by the Davis, et al. patent (U. S. Patent No. 5,633,932). With respect to applicant's claims, as amended, this rejection is respectfully traversed.

Applicant's independent claim 25 has been amended to better define applicant's invention. In particular, claim 25 recites a communication apparatus for transferring image data from a first network to a second network, said apparatus comprising: a reception unit configured to receive image data via a first network; a first discrimination unit configured to discriminate if the received image data is confidential or not; a judgment unit configured to judge if security of the transfer path to the destination of the received image data via the second network is ensured or not, when the result of the discrimination by said first discrimination unit indicates the received image data is confidential; a first control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is not confidential, to transfer the received image data to the destination of the received data via the second network regardless of whether security of the transfer path to the destination of the received image data via the second network is ensured or not; and a second control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is confidential, to transfer the received image data to the destination of the received data via the second network when the result of the judgment by said judgment unit indicates security of the transfer path is ensured, and to store the received image data in a storage area corresponding to the destination of the received image data without

transferring the received image data to the destination when the result of the judgment by said judgment unit indicates security of the transfer path is not ensured. Claims 27 and 28 have been similarly amended.

As can be appreciated from the above, the present invention as recited in amended independent claims 25, 27 and 28 is directed to a communication apparatus by which image data received via a first network is transferred to a destination through a second network.

In particular, in the present invention, as recited,

(1) if the received image data is not confidential, the received image data is transferred via the second network irrespective of whether or not security of a transfer path via the second network is ensured, and

(2) if the received image data is confidential,

(2-1) the received image data is transferred via the second network if security of the transfer path via the second network is ensured, and

(2-2) the received image data is not transferred to the destination but is stored in a storage area corresponding to the destination if security of the transfer path via the second network is not ensured.

Accordingly, in the recited invention, if the received image data is confidential, the confidentiality of the received image data can effectively be protected.

More specifically, if the received image data is not confidential, it is unnecessary to change a transfer process according to whether or not security of the transfer path via the second network has been ensured. Accordingly, the received image data is transferred irrespective of whether or not security of the transfer path via the second network has been ensured. On the

other hand, if the received image data is confidential, it is necessary to change a transfer process according to whether or not security of the transfer path via the second network has been ensured. This is because there is a concern that the content of the image data may be leaked if the confidential image data is transferred via a path of the second network for which security of such transfer path has not been ensured.

In consideration of the above, in the claimed invention, if the received image data is confidential, it is judged whether or not security of the transfer path via the second network has been ensured. The received image data is then transferred if it is judged that security of the transfer path via the second network has been ensured. On the other hand, the received image data is stored in the storage area without transferring it if it is judged that security of the transfer path via the second network is not ensured.

Thus, in the claimed invention, even in the case where the received image data is confidential, the received image data is transferred if security of the transfer path via the second network has been ensured. On the other hand, the received image data is not transferred if the received image data is confidential and security of the transfer path via the second network is not ensured. It is, therefore, possible to prevent the confidential contents of the image data from being leaked.

Such a construction is not taught or suggested by the Davis, et al. patent. More particularly, the Davis, et al. patent discloses a system and method having a sending node, a printing node and a communication link coupling these nodes together in network fashion. In the system of the Davis, et al. patent when the sending node transmits a sensitive document to the printing node for printing, such printing is prevented at the printing node so as to inhibit

outputting the sensitive document until and unless an intended recipient is authenticated. More specifically, in the system of the Davis, et al. patent (column 6, lines 9-48 and FIG. 3), if a document is sensitive, the information indicating such a fact is stored in the Header on the side of the sending node and then transmitted to the printing node. Then, on the side of the printing node, it is determined based on the information of the Header whether or not the document is sensitive (Step 340). If it is determined that the document is not sensitive, the document is printed as is. On the other hand, if it is determined that the document is sensitive, the document is stored in a memory (Step 345), and then the document is printed if the recipient is authenticated (YES in Step 350).

Accordingly, in the Davis, et al. patent, the printing node discriminates whether or not the received image data is sensitive based on the information in a Header transmitted from the sending node. If not sensitive based on the Header information, the image data can be printed. If sensitive, the image data is stored and can be printed only when the recipient is authenticated.

However, in the aforesaid operation in the Davis, et al patent, there is no judging if the security of the transfer path to the destination of the received image data via the second network is ensured or not, let alone that such judging be used to permit or disallow transfer of the received image data. In fact, the operation disclosed in FIG. 3 of the Davis, et al. patent does not concern the details of how the received document or image data is transferred. That is, this figure in the Davis, et al. patent merely discloses that the received document is printed but does not show the details of how the document is transferred.

Moreover, as discussed above, the Davis, et al. patent aims to authenticate, on the printing node, whether or not to be able to print the sensitive document, that is, to authenticate

whether or not the user who is operating the relevant printing node is the intended recipient. In other words, the Davis, et al. patent aims to limit or eliminate the user of the printing node who intends to unfairly access the already stored sensitive document.

On the other hand, in applicant's claimed invention, whether or not to transfer the image data via the second network to the destination is controlled and this control is brought about according to whether or not security of the transfer path on the second network has been ensured. This is based on the possibility that many unspecified uses can access the relevant transfer path. The claimed invention thus aims to eliminate the possibility of unfairly accessing, through the transfer path, a confidential document not yet transferred. This is quite different from the above-discussed operation in the Davis, et al. patent.

Thus, it is submitted that the feature of applicant's claimed invention of judging whether or not security of the transfer path to the destination of the received image data via the second network has been ensured is not taught or suggested by the above-cited passages of the Davis, et al. patent which do not disclose even the details of the operation of transferring the received image data. Moreover, it follows that the feature of the present invention of controlling whether to transfer the received image data or store the received image data without transferring based on such judging cannot be taught or suggested by such passages of the Davis, et al. patent which do not teach or suggest the judging.

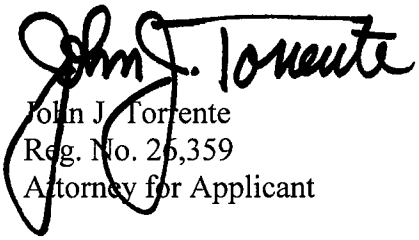
Applicant's amended independent claims 25, 27 and 28, and their respective dependent claims in reciting, in one form or another, " . . . a judgment unit configured to judge if security of the transfer path to the destination of the received image data via the second network is ensured or not, when the result of the discrimination by said first discrimination unit indicates the

received image data is confidential; a first control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is not confidential, to transfer the received image data to the destination of the received data via the second network regardless of whether security of the transfer path to the destination of the received image data via the second network is ensured or not; and a second control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is confidential, to transfer the received image data to the destination of the received data via the second network when the result of the judgment by said judgment unit indicates security of the transfer path is ensured, and to store the received image data in a storage area corresponding to the destination of the received image data without transferring the received image data to the destination when the result of the judgment by said judgment unit indicates security of the transfer path is not ensured", thus patentably distinguish over the Davis, et al. patent.

In view of the above, it is submitted that applicant's claims, as amended, patentably distinguish over the cited art of record. Accordingly reconsideration of the claims is respectfully requested.

Dated: May 19, 2008

Respectfully submitted,



COWAN, LIEBOWITZ & LATMAN
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200

John J. Torrente
Reg. No. 26,359
Attorney for Applicant